Infoblox
NEXT LEVEL NETWORKING

Infoblox 全面的 DDI 方案

该告别微软和 BIND 了

在许多组织中，支持可靠连接和访问互联网的核心服务是基于免费和看似免费的产品。虽然价格可能很诱人，但这些产品往往伴随着功能性限制和管理效率低下的隐性成本。在规划增长和变化（在当今网络中不可避免）时，必须考虑“免费”的固有限制以及如何通过升级核心网络服务来增强网络。

DNS, DHCP 和 IPAM 简史

最初，DNS 是一种访问网站和应用程序的便捷方法，而 DHCP 几乎闻所未闻。它们通常由了解它们的人员进行管理，并依赖于“免费”系统，如 BIND/DHCPD 和 Microsoft DNS/DHCP。有时，电子表格是维护基本协议服务（即 DNS 和 DHCP）的基础。这些系统往往伴随着由专家小组维护的“DIY”工具而演变。当这些专家转到其他角色或其他组织时，这会阻碍运营和规划决策。

IP 地址管理 (IPAM) 是后来的一项增强型功能，有时与管理 DNS 和 DHCP 的人员脱离开来。分配资源和定义网络的团队并不是管理和定义名称和地址的人员。

在整体 IT 策略中，这些系统的业务影响或可靠性常常被忽略，对于由哪个组（操作、系统或网络）负责维护，很少有一致的规则。直到最近，将 DNS、DHCP 和 IPAM 三者结合起来的概念（“DDI”）才被采纳。

现代网络中的 DDI

随着在过去 20 年中网络和移动出现了难以置信的增长，对其依赖性也越来越高，移动设备的使用也随之激增，DNS 现在就好比是一种“拨号音”服务，被认为可以全天候运行。

现在对于身份验证、数据库和其他后端资源、IPv6、物联网等几乎所有东西的迫切访问需求将 DDI 推向了网络的核心位置。这给极端可靠性、集成和责任性带来了额外的要求。原始设计模型中从未充分考虑过这些内容。

虽然免费或开源解决方案可以提供所需的服务，但它们可能需要大量的维护，并且缺乏当今现代网络中被视为“企业级”的稳健性。

企业也正在转向更加自动化的环境，特别是在云和虚拟空间中。然而，如果这些现有的解决方案想要适应预期的自动化水平，则需要进行更多定制。随着 IPv6 越来越普遍，通过电话读取 IP 地址的日子也一去不复返，这种困难将进一步增加。为了妥善管理这些日益复杂的环境，必须提供可支持、可扩展、可集中管理的 DDI 解决方案。

简而言之，如果 DDI 服务中断，或者更改执行时间太长，业务功能就会受到负面影响，最终导致生产力和利润的损失。

C 级优先级

毕马威 (KPMG) 最近的一份报告列出了 CIO 的五个执行战略重点：

- 加快上市速度
- 业务数字化
- 变得更加数据驱动
- 建立公众信任
- 实施颠覆性技术

在 DDI 领域，这些可以制定为诸如“保护业务安全”、“提高业务速度”或“保护公司声誉”等行动。

在重新设计 DDI 基础设施以处理诸如此类的行动时，无需花费太多精力就可以将这些问题联系起来，并发现传统解决方案与现代集成解决方案的局限性。

只有充分保护数据和减少攻击数据的所有可能途径，才能保证业务安全，而 DNS 现在是 78% 的应用层攻击 (DDoS) 和 91% 的恶意软件传播、命令和控制以及数据泄露的主要渠道。

只有当网络核心使用的系统能够处理基础架构的合规性和保护问题、减少恶意软件以及遏制集中式威胁和解决运营模式问题时，才能实现公司的声誉和朝向更加数据驱动的业务发展。

而且，只有当 DDI 自动化到能够支持基于云的基础设施所需要的快速且可变的增长时，业务的速度才会是可行的。

实现下一代数据中心愿景的道路可能很困难。传统的 DNS 基础架构和管理电子表格中的 IP 地址无法为工作负载配置提供效率、可见性或自动化 - 使 IT 部门需要通过手动、耗时的流程来配置核心网络服务。真正的数据中心转型不仅仅是存储和计算自动化，组织还需要网络自动化来实现敏捷、集中管理且高度可扩展的数据中心。

您需要知道所有设备所处的位置、它们正在执行的操作、通信对象是谁、它们如何随着时间的推移而变化，以及手头有限的资源应该集中在哪里。

理想的系统

在如今的环境中，DDI 必须满足以下几个重要指标：

- 可靠的正常运行时间
- 易于改变
- 实时端点和拓扑可见性
- 与自动化系统集成
- 冗余和/或快速恢复时间

因此，理想的系统应该集中管理，需要最少的资源进行维护，易于部署和扩展。它还应该是稳定、安全的，并支持各种不同的需求。这些可能是高级管理员、站点/桌面支持、自动化任务、网络规划和安全取证。

对于规划和取证来说，关键是“单一事实来源”。系统必须提供一个可以查找任何设备或网络信息的地方，而不是搜索多个可能冲突或不同步的系统。

这也必须包括历史增长模式、DNS 使用和趋势的可见性、DHCP 租约记录和设备记录。所有这些都是能够快速响应安全事件、解决网络问题和总体容量规划的关键所在。

理想的解决方案还能够作为更大的生态系统的一部分与其他系统进行交互，并相互动态通信以交换信息。而自动化现在是必须的。

此类示例包括：

- 查询已被标记为具有潜在恶意的 DNS 记录，DNS 可以通过响应策略区域“捕获”此记录。然后可以将该匹配传送到一个设备扫描仪，自动扫描所讨论的系统中可能出现的问题，并在必要时发出警报，隔离所述系统。
- DHCP 租约日志可以发送到第三方日志系统，以跟踪使用趋势和事件相关性
- 为新建的 VM 提供 IP 分配和回收的自动化系统可以将配置时间从数小时或数天缩短至数分钟。
- 标记恶意端点的端点安全系统可以自动将此信息推送到安全策略中，以防止客户端联系所述端点。

当然，这些只是众多示例中的一小部分，在这些示例中，系统之间的自动交互可以实现易于更改、实时端点和拓扑可见性以及与自动化系统的集成。

Infoblox 的优势

传统系统无法扩展

尽管 BIND 在 DNS 和互联网方面已成为行业标准，但它需要高水平的知识和技能才能正确实施和运行。正确执行简单任务涉及多个手动步骤（例如，添加/修改/删除记录时，区域的序列号必须递增）。在实现更复杂的配置和功能（如 DNSSEC）时，存在一些缺陷，可能导致不可预测的性能问题，甚至可能导致 DNS 完全中断。

此外，虽然 BIND 支持 DNS，但它没有提供支持性能监视和管理的集成报告，也没有提供与 IP 地址管理的集成，这导致本地 DNS 记录与 IPAM 中可能出现的内容之间存在差异。BIND 从未在自动化的基础上进行过开发，因此它没有用于简单自动化 DNS 记录更改的强大 API，而 DDI 系统却可以提供这一点。

将 IPAM 与 DNS 集成

将 IPAM 与 DNS 集成对于保持两个系统的准确性和同步性至关重要。当在网络上部署新设备时，首先要分配IP 地址，然后通常紧接着是将主机添加到 DNS 的请求。通过集成 DNS 和 IPAM，此过程变成了一个步骤 - 在 IP 分配的同时创建 DNS 记录。这不仅可以提高效率，还可以降低错误发生的可能性，因为数据不会被转录或转发。随着 IPv6 的普及，对集成 IPAM 与 DNS 的需求不断增加。

为了进一步提高 DNS 和 IPAM 的准确性，可以添加一个发现组件。将发现组件集成到 IPAM 中可以将其从几乎完全依赖于人工操作的系统转换为“权威 IPAM”，使网络管理员和安全操作人员可以随时查看网络上的实时内容。与报告解决方案结合使用时，可以按照时间跟踪 IP 地址的历史记录，这对于正确分析安全事件至关重要。

Infoblox DDI 让您可以使用现代 DNS 服务系统，通过以下方式解决许多问题：

- 将 DNS、DHCP、IP 地址管理和其他核心网络服务整合到一个平台中，通过通用控制台进行管理
- 利用集成功能，为混合云、公共云、虚拟和私有云环境集中协调横跨各种基础架构的 DDI 功能
- 访问丰富的集成报告和分析功能，用于容量规划、资产管理、法规遵循控制和审计
- 通过 RESTful API 与 Infoblox Grid 结合，与其他 IT 系统无缝集成，提高IT效率和自动化程度

用于 DNS 的 Infoblox 与 Microsoft DNS 的比较

在选择与 Microsoft Active Directory 一起使用的 DNS 解决方案时，许多管理员只是简单地选择 Windows Server 随附的解决方案。然而，有很多理由证明可以使用非 Microsoft DNS。

- 安全：组织需要最好的解决方案，因为它们的外部 DNS 暴露于网络攻击之下。提供基于安全考虑而设计和构建的第三方 DNS 解决方案。组织的内部 DNS 结构同样容易受到恶意威胁、恶意软件、网络钓鱼和数据泄露的危害。
- 可见性和单一视图：大多数组织都拥有异构的技术组合。准确的一站式可见性对于高效的合规性和控制来说是必不可少的。
- 运营效率：利用自动化和工作流程取代手动电子表格进行管理，从而优化运营支出。
- 情报服务：集成的基于 DNS 的流量控制、网络负载平衡和服务监控为组织增加了巨大的价值。Microsoft IPAM 中的差距会在当前网络拓扑状态与 Microsoft Active Directory (AD) 中包含的信息之间造成不一致。这可能导致用户身份验证和文件可用性等基本服务完全中断。

Infoblox IPAM 还可以与 Microsoft AD 站点和服务无缝集成，弥补 AD 和网络管理员之间的差距。此外，Infoblox 跨越了微软实例集，将整个微软环境引入一个集中管理的 GUI 中，提供前所未有的可见性、运营效率和服务正常运行时间。

欲了解更多信息，请参阅“微软 vs 非微软 DNS：事实与虚构，”一文，作者是 Jeremy Moskowitz，集团政策 MVP。

Infoblox 与其他产品及生态系统的集成

Infoblox 还可以与领先的安全和管理技术实现无缝集成。我们通过开放 API 实现情报自动化，并支持跨云和本地环境的工作负载。我们的产品包括具有高级威胁情报和生态系统集成的上下文感知安全性。

作为更大的安全生态系统的一部分，Infoblox 还支持 REST 和 PERL API，以及基于事件的 Outbound API，它可以与安全基础架构中的其他系统交互，添加网络以便在它们被添加到 IPAM 时进行扫描，如果终端设备发送与 RPZ 规则匹配的查询（包括威胁洞察）等，则会触发设备扫描和/或隔离。此外，Infoblox 还与 Cisco ISE、McAfee 及其他 20 多家公司进行了整合，而且这一数字还在不断增长。

结论

您应采取的措施

“免费”系统，如 BIND/DHCPD、Microsoft DNS/DHCP 和电子表格等，无法充分满足现代网络的需求。花时间检查核心部分的弱点，并制定一个计划，将其迁移到集成的 IPAM 系统。

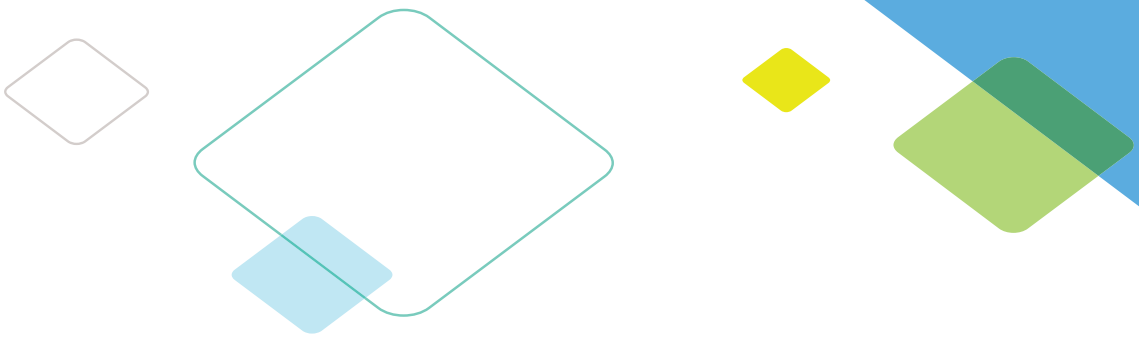
确定您现有的工作流程和 IPAM 流程，看看您可以在哪些方面进行改进：

- 可靠的正常运行时间
- 易于改变
- 实时端点和拓扑可见性
- 与自动化系统集成
- 冗余和/或快速恢复时间

Infoblox 拥有良好的业绩记录，是市场领导者，市场占有率超过 50%，拥有 8,000 多名客户，我们有许多资源可以帮助您做出这一决定：
https://www.infoblox.com/resources/?category=Whitepapers

接下来的步骤

联系您的 Infoblox 销售团队，讨论建议的部署体系结构。



Infoblox 安全的云管理网络服务，引领着下一代 DDI 的发展。Infoblox 服务让本地、云和混合网络的安全和自动化水平以及可靠性都再上一个台阶，为客户铺好单一网络管理平台的大道。Infoblox 是公认的行业领导者，市场占有率达 50%，客户 8,000 多家，其中 350 家位列《财富》500 强。

公司总部 | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256（美国和加拿大免费电话）| info@infoblox.com | www.infoblox.com